UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/828,695	04/05/2001	Ernie F. Brickell	10559/458001/P10869	6460

20985 7590 05/17/2006

FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
CALLAHAN, PAUL E	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 05/17/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/828,695	**Applicant(s)** BRICKELL	
	Examiner Paul Callahan	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 February 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,12-19,21-28,31 and 32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *18,19,21,22 and 32* is/are allowed.

6)☐ Claim(s) *1,4,9,10,16,17,23,25,28 and 31* is/are rejected.

7)☐ Claim(s) *2,3,5-8,12-15,24,26 and 27* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 February 2006* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-10, 12-19, 21-28, 31 and 32 are pending in this application and have been examined.

2. The indicated allowability of Claims 1-10, 12-17, 23-28, and 31 is withdrawn in view of the newly discovered reference(s) to Arthan US 6754,349. Rejections based on the newly cited reference(s) follow.

Drawings

3. The drawing replacement sheets were received on 2-7-06. These drawings are not acceptable because of the following informalities:

Fig. 2 has a handwritten notation on the face of the drawing stating that: "For the sake of consistency, all K's have been capitalized" In order to avoid abandonment of this application; correction is required in reply to the Office action. The correction will not be held in abeyance.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 4, 9, 10, 16, 17, 23, 25, 28, and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Arthan.

As for Claim 1, Arthan teaches a method comprising; defining a key and a set of values the key able to be derived using the values and a predefined relationship between the values (col. 1 lines 15-20: generation of a recovery key from secret information and a key generation value, col. 3 lines 5-10), sending a second value of a set but not all of the values of the set to a first delegate (col. 1 lines 20-23: the secret information, in this case a key, is sent to a key server which reads on the "delegate" of the applicant's Claim), and wherein the encrypted information is inaccessible without both the first and second values of the set (col. 1 lines 20-25: both the recovery key generation value and the secret information are required to generate a recovery key used to decrypt the encrypted information). Arthan does not explicitly teach sending a first value of the set, but not all values of the set, and the encrypted information to a server for storage. However Arthan does teach storage of the values a one of a plurality of client computers connected to a network (col. 1 lines 19-22: the recovery key and secret information encrypted under the recovery key is held at a first location, this is taught as one of a plurality of client computers in col. 2 lines 5-35). Official Notice can be taken that such an arrangement of a client computer, which serves as a network node, can also serve as a network server. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Arthan. It would have been desirable to do so as this would facilitate rapid transmission of a recovery key and recovery of encrypted data on a client's system.

As for Claim 4, Arthan teaches a set that includes exactly two values (col. 1 lines 15-30: the secret information and the recovery key generation value are the two values).

As for Claim 9, Arthan does not teach the use of encrypted information that is medical information. However Official Notice may be taken that the use of such a system in the secure storage of medical information is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Arthan. It would have been desirable to do so as this would increase the utility and hence marketability of the system.

As for Claim 10, Arthan teaches a method comprising, storing secured information and a first access component, access to the secured information requiring a key (col. 1 lines 20-22: storing the secured information and the recovery key generation value at the first location) the key able to be derived using the first access component and a second access component and a relationship between them (col. 1 lines 15-25: generating a recovery key from a secret information and a recovery key generation value), excluding both the key and the second access component from the storage location (col. 1 lines 15-25 the secret information is stored at a remote server, the recovery key is not stored at the location), providing the secured information and the first access component to a first requestor (col. 2 lines 20-25). Arthan does not explicitly teach storage of the secured information and the first access component at a server. Instead Arthan teaches the use of a client computer connected to a network (col. 2 lines 25-35). However, Official Notice can be taken that such an arrangement of a client computer, which serves as a network node, can also serve as a network server. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Arthan. It would have been desirable to do so as this would facilitate rapid transmission of a recovery key and recovery of encrypted data on a client's system.

As for Claim 16, Arthan teaches the use of an authentication technique prior to provision of the information requested (col. 4 lines 45-50), but does not explicitly teach storage of authentication (permission) information. However Official Notice may be taken that the use of such stored permission information is a step that is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Arthan. It would have been desirable to do so since storage of the permission information would decrease the likelihood of such information becoming lost or unavailable.

As for Claim 17, Arthan teaches the secured information is secured by an encryption key (col. 1 lines 19-21: the secret information is encrypted using a generated recovery key), and where the first and second access components are related to the key by a predefined relationship (col. 3 lines 1-15: generation of the recovery key is via a hash function applied to the first and second access components).

As for Claim 23, the Claim is directed towards a computer program embodied in a memory medium that, when read out, causes a processor to perform the method of Claim 1. Therefore Claim 23 is rejected on the same basis as is Claim 1.

As for Claims 25 and 28, the Claims are directed towards an apparatus that carries out the methods of Claims 1 and 9 and are therefore rejected on the same basis as are those Claims.

As for Claim 31, Arthan teaches sending authentication information to the server operator, allowing the first delegate access to the first of the values (col. 3 line 25-45). Arthan does explicitly teach electronic transmission to the server itself. However Official Notice may be taken that the use of such a technique is old and well known in the art. Therefore it would have been obvious to one of ordinary skill in the art to incorporate this technique into the system of Arthan. It would have been desirable to do so as this would allow more rapid authentication techniques to be used.

Allowable Subject Matter

6. Claims 18, 19, 21, 22, and 32 are allowed.

7. Claims 2, 3, 5, 6-8, 12-15, 24, 26, 27, and 31 are objected to as being dependent upon a rejected base Claim, but would be allowable if rewritten in independent form including all of the limitations of the base Claim and any intervening Claims.

8. The following is a statement of reasons for the indication of allowable subject matter:

As for Claim 18, the prior art does not teach the combination of method steps of the Claim, particularly including receipt of the second access component from a source other than the client or the server. Claims 19-22 and 32 are dependent on Claim 18 and are therefore allowable on that basis,

As for Claim 2, the prior art does not teach the combination of method steps found in the Claim including generation of a second set of values and use of the second set in generation of a key. Claim 3 is dependent on Claim 2 and would be allowable on that basis should Claim 2 be rewritten in independent form including all of the limitations of the base Claim and any intervening Claim,

As for Claim 5, he prior art does not teach a set containing three or more values,

As for Claim 6, the prior art does not teach the descriptor of a first delegate, used in the manner of the applicant, As for Claim 7, the prior art does not teach the set of values as found in Claim 1 with probability of guessing the key using one value of the set is the same as guessing with knowledge of no values of the set. Claim 8 is dependent on Claim 7 and would be allowable on that basis should Claim 7 be rewritten in independent form including all of the limitations of the base Claim and any intervening Claim,

As for Claim 12, the prior art does not teach the third and fourth access components of the applicant. Claims 13-15 are dependent on Claim 12 and would be allowable on that basis should Claim 12 be rewritten in independent form including all of the limitations of the base Claim and any intervening Claim,

As for Claim 24, the prior art does not teach generation of a second set of values and use of the second set in generation of a key in the manner of the applicant,

As for Claim 26, the prior art does not teach storage of a second set of values useful in generation of the key. Claim 27 is dependent on Claim 26 and would be allowable on that basis should Claim 26 be rewritten in independent form including all of the limitations of the base Claim and any intervening Claim.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300.

5-12-06
Paul Callahan